ZT IT-KOLUMNE

Kryptografie – Teil III

In diesem Teil geht es nun um „Digitale Zertifikate". Diese werden für eine sichere Informationsübertragung im Internet für eine Verschlüsselung von vertrauenswürdigen Daten verwendet. Dieser Artikel beschreibt nun im Detail die Funktionsweise von digitalen Zertifikaten als asymmetrisches Verschlüsselungsverfahren.

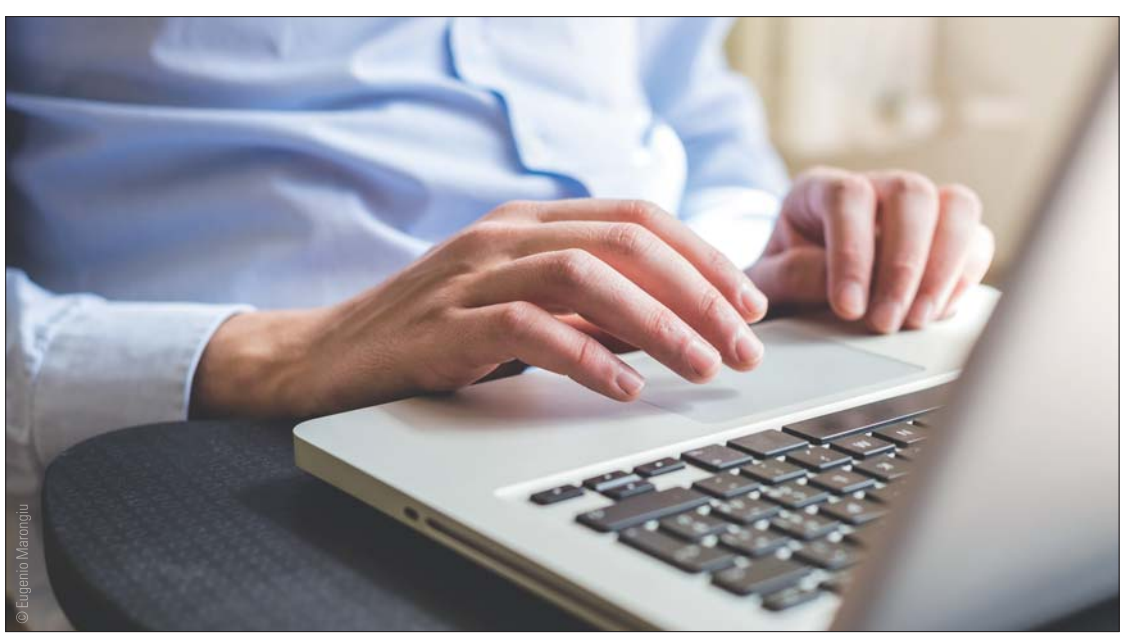
Möchten Internetnutzer Daten vertraulich versenden und empfangen, so kommen hierbei Verschlüsselungstechniken zum Einsatz. In den ersten beiden Artikeln der Kryptografie-Serie haben wir verschiedene Verschlüsselungsverfahren kennengelernt, mit dem die folgenden Ziele verfolgt werden.

Vertraulichkeit

Hier wird gefragt: Wie können die Daten so geschützt werden, dass kein anderer die Daten unerlaubt lesen kann. Die Daten müssen von den Kommunikationspartnern also „vertraulich" gesendet und empfangen werden. Das Ziel: Eine Nachricht darf nur für denjenigen lesbar gemacht werden, für den sie bestimmt ist. Genau das war schon immer der Zweck von geheimen Schriften und Verschlüsselungen.

Authentizität (Verbindlichkeit)

Unter dem Begriff „Authentizität" von Informationen *(engl. authenticity)* wird die Echtheit und Glaubwürdigkeit der Informationen verstanden, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar sind.
Das Ziel: Es dürfen keine Zweifel bestehen, dass die Herkunft der Informationen korrekt ist und die Urheber dieser Daten korrekt authentifiziert werden können.



© Eugenio Marongiu

Integrität (Unverfälschtheit)

Informationen können prinzipiell auf verschiedene Art und Weise verändert werden, z. B. durch Fehler bei der physikalischen Übertragung der Daten durch Verbindungsfehler. Um das zu vermeiden, werden sogenannte „Prüfsummen" berechnet und an die Daten angehängt. Leider können auch die Prüfsummen manipuliert werden. Informationen können absichtlich verändert bzw. manipuliert werden (inkl. Prüfsumme). Es müssen also geeignete Schutzmaßnahmen verwendet werden, mit denen die übertragenen Informationen wieder rekonstruiert werden können.
Das Ziel: Die Informationen dürfen von keiner dritten Person verändert werden.

Was sind digitale Zertifikate und wie funktionieren sie?

Digitale Zertifikate kommen bei der asymmetrischen Verschlüsselung zum Einsatz und bestätigen unter anderem, dass ein öffentlicher Schlüssel zu der Person gehört, die im Besitz des korrespondierenden privaten Schlüssels ist.
Ein digitales Zertifikat ist Teil eines kryptografisch gesicherten Verfahrens, mit dessen Hilfe sich der Besitzer des Zertifikats identifizieren kann. Mit Zertifikaten können z. B. E-Mails „unterschrieben" werden, vorausgesetzt das E-Mail-Programm unterstützt Zertifikate.
Ein digitales Zertifikat besteht aus:

- einem öffentlichen Schlüssel und
- einem privaten Schlüssel

Der *öffentliche Schlüssel* kann von jedem im Verkehr mit dem Eigentümer verwendet werden. Deswegen darf er nicht nur jedem bekannt sein, sondern soll es sogar. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. In der Regel wird der öffentliche Schlüssel nach seiner Erstellung veröffentlicht, z. B. auf einem Key-Server.
Der *private Schlüssel* wird nur vom Eigentümer verwendet. Er darf auf keinen Fall anderen in die Hände fallen. Deswegen wird er nie aus der Hand gegeben, auch nicht zur Erstellung von Zertifikaten. Der private Schlüssel ermöglicht es seinem Inhaber, digitale Signaturen zu erzeugen, sich zu authentisieren oder für ihn verschlüsselte Daten zu entschlüsseln.
Man kann sich ein Zertifikat wie einen Personalausweis in digitaler Form vorstellen: Beim Personalausweis garantiert die vertrauenswürdige Stelle „Meldeamt", dass die Unterschrift, die sich auf dem Ausweis befindet, auch tatsächlich zu der Person gehört, deren Stammdaten und Passbild sich auf dem Ausweis befinden. Im Gegensatz zum Personalausweis werden Zertifikate aber von vielen verschiedenen Zertifizierungsstellen (z. B. GobalSign, Verisign, Trust Center u. a.) und in vielen verschiedenen Qualitätsstufen ausgegeben. Es ist Sache des Benutzers zu entscheiden, ob er dem Herausgeber des Zertifikates vertraut.
Ein Zertifikat enthält Informationen über den Namen des Besitzers, dessen öffentlichen Schlüssel, eine Seriennummer, eine Gültigkeitsdauer und den Namen der Zertifizierungsstelle. Diese Daten sind in der Regel mit dem privaten Schlüssel der Zertifizierungsstelle signiert und können somit mit dem öffentlichen Schlüssel der Zertifizierungsstelle überprüft werden. Zertifikate für Schlüssel, die nicht mehr sicher sind, können über eine sogenannte Zertifizierungssperrliste gesperrt werden.
Es stellt sich also die große Frage: Wenn ich von jemandem seinen öffentlichen Schlüssel erhalte, woher weiß ich, das er wirklich von dieser Person stammt? Wenn es so einfach ist, eine falsche Identität vorzugeben, wie kann man dann jemandem VERTRAUEN, dass er der ist, der er vorgibt zu sein? Hier kommen nun die Zertifikate ins Spiel. Ein Zertifikat ist ein digitales Dokument, das die Identität und den Schlüsselbesitz eines Individuums, eines Computersystems (oder eines einzelnen Servers aus diesem System) oder einer Organisation bestätigt. Beispielsweise kann das Zertifikat eines Nutzers bestätigen, dass derjenige tatsächlich der rechtmäßige Besitzer dieses speziellen öffentlichen Schlüssels ist. Ein digitales Zertifikat wird von einer Zertifizierungsstelle *(certificate authority, CA)* ausgestellt. Diese Stelle ist dafür verantwortlich, die Identität und den Schlüsselbesitz eines Individuums vor dem Ausstellen des Zertifikates zu überprüfen.
Authentifizierung und Datenintegrität werden in einer digitalen Unterschrift vereint. Wie arbeitet eine Unterschrift nun?
Authentifizierung: Eine ganz spezielle Person hat die Nachricht gesendet (mit anderen Worten: kein Nachahmer, der vorgibt diese Person zu sein, hat sie geschickt).
Integrität: Die Nachricht wurde genauso verschickt, wie sie empfangen wurde (mit anderen Worten: niemand hat die Nachricht vor ihrem Empfang verändert). Wenn man nun z. B. eine E-Mail an eine andere Person versendet, erzeugt die private/geheime Schlüsselkombination die digitale Signatur. Die digitale Signatur macht dies auf folgende Weise:

1. Der Absender nutzt einen „Message-Digest-Algorithmus", um eine kürzere Version der Nachricht zu erzeugen, die verschlüsselt werden kann. Diese kürzere Version heißt „Message Digest" (etwa: Nachrichtenextrakt). Nachrichtenextrakte und die Algorithmen, die sie erzeugen, werden im nächsten Abschnitt erklärt.
2. Der Absender verwendet seinen privaten Schlüssel, um den Nachrichtenextrakt zu verschlüsseln.
3. Der Absender schickt die Nachricht und den verschlüsselten Extrakt nun an den gewünschten Empfänger.
4. Der Empfänger (Adressat) entschlüsselt den Extrakt.
5. Der Empfänger erzeugt auch einen Extrakt der Nachricht.

6. Der Empfänger vergleicht den selbst erzeugten Extrakt mit dem empfangenen. Sind die beiden identisch, weiß der Empfänger, dass die Nachricht von der angegebenen Person stammt und während der Übertragung im Internet nicht verändert wurde. Sind sie nicht identisch, weiß der Empfänger, dass die sendende Person nicht die ist, die sie behauptet zu sein, oder dass die Nachricht während der Übertragung verändert oder beschädigt wurde.

Der verschlüsselte Nachrichtenextrakt dient als „digitale Signatur“ der eigentlichen Nachricht. Diese garantiert für die Identität des Absenders und für den unveränderten Inhalt der Nachricht. Wird die Nachricht durch jemanden verschickt, der vorgibt jemand anderes zu sein, so hat diese Person keinen Zugriff auf den privaten Schlüssel des Absenders, den er vorgeben will zu sein. Er muss also einen anderen privaten Schlüssel verwenden, um den Nachrichtenextrakt zu verschlüsseln.
Da der Empfänger den öffentlichen Schlüssel des Absenders nutzt, um den Nachrichtenextrakt zu entschlüsseln (und nicht den eigentlichen öffentlichen Schlüssel, der zu dem privaten Schlüssel gehört, der benutzt wurde, um den Nachrichtenextrakt zu verschlüsseln) werden die beiden Extrakte, die der Empfänger erzeugt, nicht übereinstimmen. Wurde die Nachricht während deren Übermittlung verändert oder beschädigt, wird der Algorithmus beim Empfang einen anderen Nachrichtenextrakt erzeugen als beim Versenden.

Bedeutung des Status von Zertifizierungsstellen

Zertifizierungsstellen sind entweder akkreditiert oder nicht akkreditiert. Eine Zertifizierungsstelle, die das Akkreditierungsverfahren gemäß SigG erfolgreich durchlaufen hat, wird als akkreditiert eingestuft und darf gemäß § 15 Abs. 1 Satz 3 SigG ein entsprechendes Gütesiegel tragen. Die Zertifizierungsstellen werden von sogenannten Bestätigungsstellen auf technische Sicherheit und langfristige Eignung umfassend geprüft.

Zertifikatstypen nach deutschem Signaturgesetz/ EU-Richtlinie

Das deutsche Signaturgesetz (SigG) bzw. die EU-Richtlinie bewerten die Qualität von Zertifikaten in acht Stufen, von denen aber lediglich vier Stufen von Bedeutung sind:
- einfaches digitales Zertifikat
- fortgeschrittenes digitales Zertifikat
- qualifiziertes digitales Zertifikat
- akkreditiertes digitales Zertifikat

Die einfachen und fortgeschrittenen digitalen Zertifikate sind völlig unreguliert und werden vom Gesetzgeber nicht mit einer eigenhändigen Unterschrift gleichgesetzt.
Qualifizierte Zertifikaten werden mit der eigenhändigen Unterschrift gleichgestellt. Der Begriff „qualifiziertes Zertifikat“ ist eine Abkürzung für fortgeschrittene Signaturen, die mit einer sicheren Signaturerstellungseinheit erstellt wurden, die sich in der alleinigen Verfügung des Inhabers befindet. Bei qualifizierten Zertifikaten sind die gesetzlichen Vorgaben exakt. Zum Beispiel:
- biometrische Daten
- Meldeanschrift des Zertifikatinhabers

Auch spielt hierbei die Speicherung (Sicherung) des qualifizierten Zertifikats auf besonderen Medien, wie z. B. auf „SmartCards“ oder „Token“, eine entscheidende Rolle.
Die Akkreditierung bei den akkreditierten Zertifikaten bezieht sich nicht auf das Zertifikat, sondern auf die Zertifizierungsstelle. Dies ist somit kein eigener Zertifikattyp: Es sind quasi qualifizierte Zertifikate, deren Zertifizierungsstelle akkreditiert wurde.

Infos zum Autor

Ausblick

Im nächsten Artikel geht es um das Thema „Public Key Infrastruktur“, abgekürzt „PKI“. Es bleibt spannend, bleiben Sie also dran. ZT

ZT Adresse

Thomas Burgard Dipl.-Ing. (FH)
Softwareentwicklung
& Webdesign
Bavariastraße 18b
80336 München
Tel.: 089 540707-10
info@burgardsoft.de
www.burgardsoft.de
burgardsoft.blogspot.com
twitter.com/burgardsoft